

# BUNDESREPUBLIK DEUTSCHLAND



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:

103 13 271.6

Anmeldetag:

24. März 2003

Anmelder/Inhaber:

Siemens Aktiengesellschaft,  
München/DE

Bezeichnung:

Verfahren zur Fernwartung technischer  
Einrichtungen

IPC:

H 04 Q, G 05 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 09. Januar 2004  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

A handwritten signature in black ink, appearing to read "Hoß".

Hoß

## Beschreibung

### Verfahren zur Fernwartung technischer Einrichtungen

- 5 Die Erfindung betrifft ein Verfahren zur Fernwartung technischer Einrichtungen sowie ein computer-lesbares Speichermedium mit einem Programm zur Ausführung des Verfahrens auf einer Datenverarbeitungseinrichtung.
- 10 Technische Einrichtungen, wie z.B. Computer, medizintechnische bildgebende Einrichtungen, medizinische Arbeitsplätze, industrielle Anlagensteuerungen oder Fahrzeuge und Flugzeuge, werden in aller Regel durch hochspezialisierte Wartungstechniker gewartet. Wartungsmaßnahmen können dabei sowohl das Beheben von technischen Fehlern als auch das Verändern der Funktionalität umfassen. Für unterschiedliche Wartungsmaßnahmen kommen dabei häufig verschiedene Wartungstechniker zum Einsatz. Außerdem sind Wartungstechniker auf unterschiedliche technische Einrichtungen sowie auf unterschiedliche Komponenten von Einrichtungen spezialisiert.
- 15

Der hohe Spezialisierungsgrad macht die Wahl des jeweils geeigneten Wartungstechnikers von der jeweiligen Einrichtung und von der jeweils erforderlichen Wartungsmaßnahme abhängig. Um Wartungsmaßnahmen schnell und flexibel durchführen zu können, setzen sich deshalb in zunehmendem Maße Wartungsteams durch, die Wartungsmaßnahmen über Datenfernverbindungen durchführen.

- 20
- 25
- 30
- 35
- Die Fernwartung von technischen Einrichtungen bringt jedoch Probleme für die Sicherheit elektronischer Daten der technischen Einrichtungen mit sich. Zum einen muss eine Datenfernverbindung, die von einem Wartungstechniker zu einer zu wartenden Einrichtung aufgebaut werden, gegen unerlaubten Zugriff von Dritten geschützt werden. Zu diesem Zweck kann z.B. auf verschlüsselte Datenverbindungen, nicht öffentliche Datenleitungen oder passwortgeschützten Datenzugriff zurück-

gegriffen werden. In aller Regel wird der Aufbau einer Datenfernverbindung von einer technischen Einrichtungen nur dann zugelassen werden, wenn eine erfolgreiche elektronische Identifizierung des Verbindungspartners durchgeführt wurde.

5

Zum anderen bringt die Fernwartung das Problem mit sich, dass ein Wartungstechniker grundsätzlich auch Zugriff auf vertrauliche, in der zu wartenden Einrichtung gespeicherte Daten erhalten kann. Je nach den für die Wartung erforderlichen Datenzugriffsrechten des Wartungstechnikers kann eine solche Zugriffsmöglichkeit auf vertrauliche Daten ein unerwünschter Nebeneffekt sein. Die Zugriffsmöglichkeit kann aber zur Wartung auch notwendig und unerlässlich sein. Letzteres kann z.B. dann der Fall sein, wenn ein Fehlverhalten der technischen Einrichtung nur unter Zugriff auf vertrauliche Daten demonstriert werden kann.

Die vertraulichen Daten können z.B. Patientendaten, geheime Forschungspapiere, Entwicklungs-Informationen sowie Know-How oder demografische Daten sein. Die Wartung von Einrichtungen, die mit derartigen Daten arbeiten, kann den Zugriff auf diese Daten erforderlich machen, sie kann jedoch auch lediglich einen teilweisen Zugriff erforderlich machen oder ganz ohne Zugriff möglich sein. Der Umfang des erforderlichen Datenzugriffs ist anhand der beabsichtigten Wartungsmaßnahme vom Wartungstechniker im Vorfeld einer Wartungsmaßnahme abschätzbar.

Das starre Einschränken der Datenzugriffsrechte auf einen vorab abgeschätzten notwendigen Zugriffsumfang würde das Durchführen von Wartungsmaßnahmen jedoch unflexibel machen. Zudem müsste dazu auf Seiten der technischen Einrichtung ein Fachmann die Wartungsmaßnahme begleiten, der ausreichende Kenntnisse im Umgang mit der Einrichtung besitzt, um die Datenzugriffsrechte auf den vom Wartungstechniker abgeschätzten Umfang einzustellen zu können. Selbst dadurch könnte aber, wie oben angesprochen, nicht verhindert werden, dass für bestimm-

te Wartungsmaßnahmen der Zugriff auf vertrauliche Daten notwendig ist. Der Zugriff auf bestimmte vertrauliche Daten, z.B. Patientendaten, kann jedoch durch gesetzliche Bestimmungen für einen nicht für die Arbeit mit der technischen Einrichtung und den vertraulichen Daten eingestellten Mitarbeiter, also z.B. für einen firmenfremden Wartungstechniker, vollständig untersagt sein.

Herkömmliche Mechanismen zur Kontrolle von Datenzugriffsrechten weisen zum einen nicht die erforderliche Flexibilität auf, um Anpassungen der Zugriffsrechte in Abhängigkeit von einer beabsichtigten Wartungsmaßnahme durch eine nicht fachmännische Bedienpersonen auf Seiten der zu wartenden Einrichtung zu ermöglichen. Dies können in aller Regel nur Administratoren und technische Fachleute. Zum anderen bieten sie keine Möglichkeit, Zugriffe von firmenfremden Wartungstechnikern auf Daten, die aufgrund vertraglicher oder gesetzlicher Bestimmungen zu einem solchen Zugriff nicht zugelassen werden dürfen, auf legaler Basis zu ermöglichen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren zur Fernwartung technischer Einrichtungen anzugeben, das eine flexible Regulierung von Datenzugriffen durch Wartungstechniker unter Einhaltung besonders strenger gesetzlicher Einschränkungen von Datenzugriffsrechten ermöglicht.

Die Erfindung löst diese Aufgabe durch ein Verfahren sowie durch ein Speichermedium gemäß den unabhängigen Patentansprüchen.

Ein Grundgedanke der Erfindung besteht darin, ein Verfahren zur Fernwartung einer technischen Einrichtung durch einen Wartungstechniker mittels eines Wartungsrechners anzugeben, bei dem

a) in einem ersten Schritt eine Datenfernverbindung zwischen dem Wartungsrechner und der technischen Einrichtung aufgebaut wird,

b) in einem weiteren Schritt von dem Wartungsrechner eine von einem Umfang eines beabsichtigten Zugriffs auf in der technischen Einrichtung gespeicherte Daten abhängige elektronische Zugriffsinformationen an die technische Einrichtung übermittelt wird,

c) in einem weiteren Schritt von dem Wartungsrechner eine dem Wartungstechniker identifizierende elektronische Kennung an die technische Einrichtung übermittelt wird,

d) in einem weiteren Schritt durch die technische Einrichtung in Abhängigkeit von der Zugriffsinformation und der Kennung eine Zustimmung einer Bedienperson zu einem Zugriff ermittelt wird und

e) in einem weiteren Schritt von der technischen Einrichtung eine von der Ermittlung der Zustimmung abhängige elektronische Bestätigungs-Information erzeugt wird.

Das Verfahren weist den Vorteil auf, dass zunächst eine Datenfernverbindung unabhängig vom beabsichtigten Datenzugriff aufgebaut wird, die einen ersten Datenzugriff gestattet, aufgrund dessen der Umfang der beabsichtigten Wartungsmaßnahme und des damit verbundenen erforderlichen Datenzugriffs geplant werden kann. In Abhängigkeit von dieser Planung kann dann flexibel auf den beabsichtigten Datenzugriffsumfang reagiert werden, in dem über die bereits bestehende Datenfernverbindung eine Information über diesen Datenzugriffsumfang sowie eine Identifikation des Datenzugreifenden übermittelt wird, aufgrund derer die Zustimmung einer Bedienperson auf Seiten der technischen Einrichtung ermittelt werden kann.

Die Zustimmung betrifft dabei nicht das Aufbauen und den Zugriffsumfang der Datenfernverbindung als solche, sondern den beabsichtigten Datenzugriff als solchen, der durch einen bestimmten Wartungstechniker, der grundsätzlich nicht für die Arbeit mit den fraglichen vertraulichen Daten vorgesehen ist,

erfolgen soll. Eine von dieser Zustimmung abhängige elektronische Information wird darauf hin an den Wartungsrechner übermittelt, wodurch eine besondere Vereinbarung zwischen dem Wartungstechniker und der Bedienperson hergestellt werden kann, die sich auf den beabsichtigten Datenzugriff bezieht.

Das Zustandekommen dieser besonderen Vereinbarung kann so gestaltet sein, dass dadurch besonders strengen gesetzlichen Einschränkungen von Datenzugriffsrechten genügt wird. Z.B. könnte auf diese Weise ein zeitlich auf die Dauer der Wartungsarbeiten beschränktes Arbeitsverhältnis zwischen dem Wartungstechniker und der technischen Einrichtung etabliert werden, welches eine Legitimation für den Datenzugriff ermöglicht. Die Flexibilität des Datenzugriffs wird aber nicht einschränkt, da die Zustimmung nicht darin besteht, die Datenzugriffsrechte durch technische Maßnahmen entsprechend dem geplanten Wartungsumfang anzupassen und zuzulassen. Die Zustimmung hat vielmehr den Charakter einer Einverständniserklärung, die den Wartungstechniker eigens zum Datenzugriff autorisiert. Aus diesem Grund kann die Zustimmung auch von einer nicht für den Umgang mit der technischen Einrichtung fachmännischen Bedienperson gegeben werden.

In einer vorteilhaften Ausgestaltung des Verfahrens wird die Bestätigungs-Information von der technischen Einrichtung an den Wartungsrechner übermittelt. Dadurch kann die Bestätigungs-Information zeitnah zwischen beiden Beteiligten ausgetauscht werden und die Vereinbarung zu Wartungszwecken schnell zustande kommen.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden von der Bestätigungs-Information abhängige Informationen von der technischen Einrichtung ausgedruckt. Diese Informationen können z.B. in Form einer schriftlichen Vereinbarung ausgedruckt werden, die dann der Bedienperson der technischen Einrichtung unmittelbar vorliegt, um sie z.B. zu unterschreiben und an den Wartungstechniker zu faxen. Dies erlaubt das

einfache und schnelle Zustandebringen der Vereinbarung auch in Schriftform.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung  
5 wird von dem Wartungsrechner eine von einer Beendigung des Zugriffs abhängige elektronische Abschlussinformation an die technische Einrichtung übermittelt. Dadurch kann die Bedienperson der technischen Einrichtung zeitnah über das Ende der Wartungsarbeiten informiert werden. Zudem kann mit der Abschlussinformation die Beendigung einer zwischen Wartungstechniker und Bedienperson zu Wartungszwecken getroffenen Vereinbarung unmittelbar mitgeteilt und dokumentiert werden.  
10 Die Beendigung des Zugriffs kann dabei unabhängig von einem Abbauen der Datenfernverbindung erfolgen und sich lediglich  
15 auf eine bestimmte, abgeschlossene Wartungsmaßnahme beziehen.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung wird von dem Wartungsrechner eine elektronische Dokumentation von mittels des Wartungsrechners vorgenommenen Zugriffen an die technische Einrichtung übermittelt. Diese Dokumentation steht dann an der technischen Einrichtung zur Verfügung, um die Zugriffe des Wartungstechnikers auf Daten sowie auf Komponenten der technischen Einrichtung nachvollziehbar zu machen. Darüber hinaus können sämtliche Zugriffe auf vertrauliche Daten auf diese Weise dokumentiert werden, um im nachhinein vollständig rekonstruierbar zu sein. Diese Dokumentation kann insbesondere dazu dienen, strengen gesetzlichen Anforderungen an die Dokumentationen von Datenzugriffen auf vertrauliche Daten, z.B. Patientenakten, zu genügen.  
25

In einer weiteren vorteilhaften Ausgestaltung der Erfindung werden durch den Wartungsrechner elektronische Daten, die von der technischen Einrichtung an den Wartungsrechner übermittelt und von diesem gespeichert wurden, in Abhängigkeit von einer Beendigung des Zugriffs automatisch aus dem Wartungsrechner gelöscht. Dadurch kann sichergestellt werden, dass insbesondere vertrauliche Daten, z.B. elektronische Patien-

tenakten, zwar zu Wartungszwecken zugegriffen werden können, nach Abschluss der Wartung jedoch nicht an dafür nicht vorgesehenen Orten erhalten bleiben. Das Löschen der Daten kann dazu dienen, besonders strenge gesetzliche Anforderungen an

5 die Vertraulichkeit und Sicherheit solcher Daten zu erfüllen.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung wird ein Umfang eines beabsichtigten Datenzugriffs automatisch ermittelt. Dadurch kann nach Aufbau der Datenfernver-

10 bindung zwischen technischer Einrichtung und Wartungsrechner eine erste Fehlerdiagnose ohne Zugriff auf vertrauliche Daten durchgeführt werden, in Abhängigkeit von der dann eine Pla-

nung der beabsichtigten Wartungsmaßnahme erfolgt. Die War-  
tungsmaßnahme kann dabei z.B. unter Verwendung der bereits

15 aufgebauten Datenfernverbindung automatisch geplant werden,  
nachdem eine ebenfalls automatische erste Fehlerdiagnose

durchgeführt wurde. Das Verfahren kann jedoch auch teilauto-  
matisiert ablaufen, indem eine erste Diagnose von einem War-

tungstechniker vorgenommen wird, der daraufhin die von ihm  
beabsichtigten Wartungsmaßnahmen mittels des Wartungsrechners

20 plant. Die automatische Planung des Datenzugriffsumfangs er-  
folgt dann in Abhängigkeit von den Eingaben des Wartungstech-  
nikers. Der beabsichtigte Datenzugriffsumfang kann dabei z.B.  
einer von mehreren vordefinierten Stufen zugeordnet werden.

25 Dabei ist jede Stufe mit einem bestimmten Datenzugriffsrecht  
verbunden.

Weitere vorteilhafte Ausgestaltungen der Erfindung ergeben  
sich aus den unabhängigen Patentansprüchen.

30

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand  
von Figuren erläutert. Es zeigen:

FIG 1 Verfahrensschritte zur Fernwartung,

35 FIG 2 Verfahrensschritte zur automatischen Löschung von Da-  
ten im Anschluss an Fernwartungsmaßnahmen und

FIG 3 System aus Wartungsrechner und technischer Einrichtung.

In FIG 1 ist das Verfahren zur Fernwartung einer technischen  
5 Einrichtung in einzelnen Verfahrensschritten dargestellt. In Schritt 1 beginnt das Wartungsverfahren, indem z.B. ein Wartungstechniker von einer Bedienperson einer technischen Einrichtung 55 verständigt wird. Die Verständigung kann über E-Mail, Fax oder Telefon erfolgen. Sie kann auch automatisch  
10 von der technischen Einrichtung 55 bei Auftreten von Fehlern erzeugt und übermittelt werden.

In Schritt 3 baut der Wartungstechniker eine Datenfernverbindung 53 von einem Wartungsrechner 51 zu der zu wartenden  
15 technischen Einrichtung 55 auf. Die Datenfernverbindung kann dabei in einer Modemverbindung bestehen, in einer Intranet-Verbindung, einer Internet-Verbindung oder in einer sonstigen Verbindung zwischen dem Wartungsrechner 51 und der technischen Einrichtung 55. Bei der technischen Einrichtung 55 kann es sich sowohl um einen Computer als auch um eine sonstige  
20 technische Einrichtung mit elektronischer Steuerung und Datenfernverbindungsmittern handeln.

In Schritt 5 wird durch den Wartungstechniker oder den Wartungsrechner 51 eine erste Analyse der beabsichtigten Wartungsmaßnahme durchgeführt. Z.B. kann ein Fehlverhalten der technischen Einrichtung 55 analysiert werden oder eine Änderung der Konfiguration der technischen Einrichtung 55 geplant werden. Die Analyse kann durch den Wartungstechniker manuell  
25 durchgeführt werden und sich auf -Informationen stützen, die mit der Anforderung der Wartungsmaßnahmen übermittelt werden. Die Analyse kann auch automatisiert durch den Wartungsrechner 51 durchgeführt werden, der dazu Konfigurationsdaten, Nutzungsdocumentationen oder Funktionsparameter der technischen  
30 Einrichtung 55 abfragen kann.  
35

In Schritt 7 wird der Umfang der beabsichtigten Wartungsmaßnahme sowie der damit verbundene Umfang der beabsichtigten Datenzugriffe geplant. Dabei wird grundsätzlich zwischen Zugriffen auf vertrauliche Daten und auf nicht vertrauliche Daten unterschieden. Wartungsmaßnahmen, die keinen Zugriff auf vertrauliche Daten erforderlich machen, erfordern keine weiteren besonderen Vorkehrungen und können unmittelbar umgesetzt werden. Dagegen benötigen Wartungsmaßnahmen, die einen Zugriff durch den Wartungsrechner 51 auf vertrauliche elektronische Daten erforderlich machen, die besondere Zustimmung des Inhabers der elektronischen Daten oder einer zum Zugriff auf diese Daten autorisierten Bedienperson.

Die Planung des beabsichtigten Umfangs an Datenzugriffen unterscheidet also primär zwischen Zugriff auf vertrauliche und nicht vertrauliche Daten. Darüber hinaus können Zugriffe auf vertrauliche Daten in unterschiedlichem Umfang unterschieden und entsprechend ihrem Zugriffsumfang eingestuft werden. Die Einstufung kann sich zum Beispiel danach richten, ob auf Bilddaten, Textdaten, persönliche Angaben, Messdaten oder diagnostische Daten zugegriffen werden soll.

In Schritt 9 wird anhand der Planung des beabsichtigten Datenzugriffs unterschieden, ob auf vertrauliche Daten zugegriffen werden soll.

Falls nicht auf vertrauliche Daten zugegriffen werden soll, kann unmittelbar mit dem unten beschriebenen Schritt 19 mit den beabsichtigten Wartungsmaßnahmen fortgefahrene werden.

Falls auf vertrauliche Daten zugegriffen werden soll, wird in Schritt 11 eine elektronische Information vom Wartungsrechner 51 an die technische Einrichtung 55 übermittelt, die vom beabsichtigten Datenzugriffsumfang abhängig ist. Diese Information kann z.B. in Angaben zu den zuzugreifenden Daten sowie zu der Art der Datenzugriffe bestehen. Sie kann jedoch auch in einer Vereinbarung über die beabsichtigten Datenzugriffe

in der Art bestehen, dass ein Vertragsentwurf übermittelt wird, der die vertragliche Zustimmung der Bedienperson zu einem Zugriff des Wartungstechnikers auf die vertraulichen Daten beinhaltet. Ein solcher Vertrag könnte z.B. die Einrichtung eines vorübergehenden - auf die Dauer der Wartungsarbeiten beschränkten - Arbeitsverhältnisses zwischen dem Wartungstechniker und der technischen Einrichtung beinhalten.

In Schritt 12 wird eine elektronische Kennung, die den Wartungstechniker identifiziert, vom Wartungsrechner 51 an die technische Einrichtung 55 übermittelt. Die Kennung kann entweder den Wartungstechniker individuell und eindeutig identifizieren, oder sie kann z.B. die Rolle des Wartungstechnikers angeben.

In Schritt 13 zeigt die technische Einrichtung 55 einer Bedienperson über ein Anzeigegerät, z.B. einen Bildschirm, Informationen zum beabsichtigten Wartungszugriff und zur Identität oder Rolle des Wartungstechnikers an. Die Anzeige besteht in einer bevorzugten Ausführungsform in einem PopUp-Fenster, das eine Vereinbarung anzeigt, die den Wartungstechniker für den Datenzugriff im beabsichtigten Zugriffsumfang autorisiert.

Der Wortlaut dieser Vereinbarung kann entweder vom Wartungsrechner 51 übermittelt worden sein, oder er kann auf Seiten der technischen Einrichtung 55 verfügbar sein. Dabei kann der Inhalt der Vereinbarung in Abhängigkeit vom beabsichtigten Datenzugriffsumfang variabel, z.B. in Form einer Formularvorlage, festgelegt werden oder es kann eigens für jeden Datenzugriffsumfang eine Standardvereinbarung, z.B. in Form einer Dokumentvorlage, verfügbar sein. In einer weiteren Ausführungsform kann einer Bedienperson anstelle einer Vereinbarung lediglich eine Information über den Umfang des beabsichtigten Datenzugriffs sowie den Wartungstechniker bzw. dessen Rolle mitgeteilt werden.

In Schritt 15 erhält die Bedienperson der technischen Einrichtung 55 die Möglichkeit, dem beabsichtigten Datenzugriff zuzustimmen oder ihn abzulehnen. Die Entscheidung kann durch Eingabe der Zustimmung oder Ablehnung z.B. mittels Tastatur oder Maus direkt am Anzeigegerät der technischen Einrichtung 55 getroffen werden. In einer anderen Ausführungsform kann die Entscheidung dadurch getroffen werden, dass die im vorhergehenden Schritt gezeigten Informationen bzw. die Vereinbarung durch die technische Einrichtung 55 ausgedruckt und von einer Bedienperson in Schriftform bestätigt werden.

Falls die Bedienperson keine Zustimmung zu dem beabsichtigten Datenzugriff gibt, so wird die geplante Wartungsmaßnahme im unten beschriebenen Schritt 27 abgebrochen.

Falls die Bedienperson ihre Zustimmung zum Datenzugriff gegeben hat, so wird in Schritt 17 ein von dieser Zustimmung abhängiges elektronisches Signal erzeugt, dass von der technischen Einrichtung 55 entweder unmittelbar an den Wartungsrechner 51 übermittelt wird, oder das Erzeugen eines Ausdrucks bewirkt, der dann z.B. gefaxt werden kann.

Falls die Zustimmung der Bedienperson unmittelbar am Bildschirm der technischen Einrichtung 55 eingegeben wurde, erfolgt die Übermittlung über die Datenfernverbindung 53 und kann dem Wartungstechniker unmittelbar angezeigt werden.

Falls die Zustimmung auf einem Ausdruck schriftlich gegeben wurde, kann sie per Fax übertragen oder per Post geschickt werden. In diesem Fall erhält der Wartungstechniker die Zustimmung bzw. die vertragliche Vereinbarung für den beabsichtigten Wartungszugriff nicht genauso zeitnah wie bei der Übermittlung über die Datenfernverbindung 53. Diese Möglichkeit kann allerdings für Dokumentationszwecke genutzt werden, um Vereinbarungen bzw. Zustimmungen zu Datenzugriffen z.B. zentral zu archivieren.

In Schritt 19 nimmt der Wartungstechniker mittels des Wartungsrechners 51 Wartungsmaßnahmen über die bereits aufgebauten Datenfernverbindung 53 vor. Er hält dabei den zuvor durch die Bedienperson der technischen Einrichtung 55 im bestätigten Datenzugriffsumfang ein, um sich im zuvor geregelten Rahmen des Datenzugriffs zu bewegen. Die Datenfernverbindung 53 muss zu diesem Zweck nicht angepasst und in ihren Zugriffsmöglichkeiten technisch eingeschränkt werden, stattdessen hält der Wartungstechniker den vereinbarten Zugriffsumfang von sich aus ein.

Die Wartungsmaßnahmen des Wartungstechnikers werden in einem Dokumentationsspeicher 21 in geeigneter Weise gespeichert, um im nachhinein jederzeit vollständig rekonstruierbar zu sein.

In Schritt 23 werden die zu Dokumentationszwecken im Dokumentationsspeicher 21 gespeicherten Informationen vom Wartungsrechner 51 an die technische Einrichtung 55 übertragen. Damit kann insbesondere gesetzlichen Auflagen zur vollständigen Dokumentation von Datenzugriffen auf vertrauliche Daten genüge getan werden.

In Schritt 25 erfolgt die Beendigung der Wartungsmaßnahme entweder automatisch durch den Wartungsrechner 51 oder manuell durch den Wartungstechniker. Die Beendigung der Wartungsmaßnahme ist dabei nicht identisch mit dem Abbauen der Datenfernverbindung 53, sie bedeutet lediglich das Abschließen der zuvor geplanten und durchgeföhrten Wartungsmaßnahme. Sollte sich z.B. im Lauf der Durchführung dieser Wartungsmaßnahme herausstellen, dass ein Datenzugriff in geändertem Umfang erforderlich wird, so kann eine laufende Wartungsmaßnahme abgebrochen und eine Wartungsmaßnahme in dem erforderlichen, geänderten Zugriffsumfang eingeleitet werden.

In Schritt 27 wird einer Bedienperson durch die technische Einrichtung 55 die Beendigung der Wartungsmaßnahme angezeigt. Die Beendigung der Wartungsmaßnahme ist gleichbedeutend, dass

die Zustimmung der Bedienperson zu einem Datenzugriff im zuvor festgelegten Umfang erlischt. Erfolgte die Zustimmung im Rahmen einer vertraglichen Vereinbarung, so ist die Beendigung der Wartungsmaßnahme in Schritt 27 mit der Kündigung der vertraglichen Vereinbarung identisch. Zu diesem Zweck kann der Bedienperson z.B. eine mit der vorangehenden Vereinbarung konforme Kündigung als PopUp-Fenster auf einem Bildschirm der technischen Einrichtung 55 angezeigt werden.

- 10 In Schritt 29 wird nach Beendigung sämtlicher Wartungsmaßnahmen die Datenfernverbindung 53 abgebaut und in Schritt 31 das Wartungsverfahren beendet.

15 In **FIG 2** ist das Verfahren zum Löschen vertraulicher Daten vom Wartungsrechner 51 dargestellt. In Schritt 19 erfolgt dabei, wie zuvor beschrieben, die Durchführung von Wartungsmaßnahmen und deren Speicherung zu Dokumentationszwecken im Dokumentationsspeicher 21. In Schritt 23 werden, wie ebenfalls zuvor beschrieben, die zu Dokumentationszwecken gespeicherten 20 Informationen an die technische Einrichtung 55 übertragen.

25 In Schritt 24 erfolgt unter Verwendung der zu Dokumentationszwecken gespeicherten Informationen das Löschen sämtlicher Daten, die während der Wartungsmaßnahmen von der technischen Einrichtung 55 an den Wartungsrechner 51 übertragen wurden und von diesem gespeichert wurden. Die Verwendung der Dokumentationsinformationen ermöglicht dabei das vollständige Löschen, so dass im Anschluss gewährleistet ist, dass keine vertraulichen Daten auf Seiten des Wartungsrechners 51 erhalten 30 bleiben.

- In Schritt 25 erfolgt, wie zuvor beschrieben die Beendigung der Wartungsmaßnahme von Seiten des Wartungsrechners 51.
- 35 In Schritt 26 wird der Bedienperson der technischen Einrichtung 55 im Anschluss an die Beendigung der Wartungsmaßnahme das zuvor in Schritt 24 erfolgte erfolgreiche Löschen sämtlich-

cher vertraulicher Daten auf Seiten des Wartungsrechners 51 bestätigt.

In Schritt 27 wird, wie zuvor beschrieben, durch die technische Einrichtung 55 die Beendigung der Wartungsmaßnahmen in Form einer Aufkündigung der zuvor getroffenen Vereinbarung angezeigt.

In FIG 3 ist ein System zur Wartung einer technischen Einrichtung 55 dargestellt. Die technische Einrichtung 55 kann dabei z.B. ein Computer oder eine Computersteuerung einer Einrichtung sein. Ein Wartungsrechner 51, z.B. ein Computer oder ein Notebook, wird mit der technischen Einrichtung 55 über eine Datenfernverbindung 53 verbunden. Die Datenfernverbindung 53 kann dabei in einer Modemverbindung, einer Intranet-Verbindung, einer Internet-Verbindung oder sonstigen Datenverbindungen bestehen. Eine weitere technische Einrichtung 55 ist beispielhaft dargestellt, die ebenfalls Zugriff auf eine Datenfernverbindung 53 hat, jedoch nicht mit dem Wartungsrechner 51 verbunden ist.

Die zur Ausführung des Verfahrens auf einer Datenverarbeitungseinrichtung notwendigen Informationen können auf einem computer-lesbaren Speichermedium gespeichert sein. Das Speichermedium kann z.B. eine Diskette, ein Disketten-Paket, eine Festplatte, ein Server sein. Die darauf gespeicherten Informationen können mit einer Datenverarbeitungseinrichtung in Wechselwirkung treten, um z.B. das Verfahren auf der Datenverarbeitungseinrichtung auszuführen oder ein zur Ausführung benötigtes Programm darauf zu installieren.

## Patentansprüche

1. Verfahren zur Fernwartung einer technischen Einrichtung (55) durch einen Wartungstechniker mittels eines Wartungsrechners (51), bei dem a) in einem Schritt (3) eine Datenfernverbindung (53) zwischen dem Wartungsrechner (51) und der technischen Einrichtung (55) aufgebaut wird, b) in einem Schritt (11) von dem Wartungsrechner (51) eine von einem Umfang eines beabsichtigten Zugriffs auf in der technischen Einrichtung (55) gespeicherte Daten abhängige elektronische Zugriffs-Information an die technische Einrichtung (55) übermittelt wird, c) in einem Schritt (12) von dem Wartungsrechner (51) eine den Wartungstechniker identifizierende elektronische Kennung an die technische Einrichtung (55) übermittelt wird, d) in einem Schritt (15) durch die technische Einrichtung (55) in Abhängigkeit von der Zugriffs-Information und der Kennung eine Zustimmung einer Bedienperson zu einem Zugriff ermittelt wird und e) in einem Schritt (17) von der technischen Einrichtung (55) eine von der Ermittlung der Zustimmung abhängige elektronische Bestätigungs-Information erzeugt wird.
2. Verfahren nach Anspruch 1, bei dem die Bestätigungs-Information von der technischen Einrichtung (55) an den Wartungsrechner (51) übermittelt wird.
3. Verfahren nach einem der vorhergehenden Ansprüche, bei dem von der Bestätigungs-Information abhängige Informationen von der technischen Einrichtung (55) ausgedruckt werden.
4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem in einem Schritt (25) von dem Wartungsrechner (51) eine von einer Beendigung des Zugriffs abhängige elektronische Abschluss-Information an die technische Einrichtung (55) übermittelt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem  
in einem Schritt (23) von dem Wartungsrechner (51) eine e-  
lektronische Dokumentation von mittels des Wartungsrechners  
(51) vorgenommenen Zugriffen an die technische Einrichtung  
5 (55) übermittelt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem  
in einem Schritt (24) durch den Wartungsrechner (51) elektro-  
nische Daten, die von der technischen Einrichtung (55) an den  
10 Wartungsrechner (51) übermittelt und von diesem gespeichert  
wurden, in Abhängigkeit von einer Beendigung des Zugriffs au-  
tomatisch aus dem Wartungsrechner (51) gelöscht werden.

15 7. Verfahren nach einem der vorhergehenden Ansprüche, bei dem  
in einem Schritt (7) ein Umfang eines beabsichtigten Daten-  
zugriffs automatisch ermittelt wird.

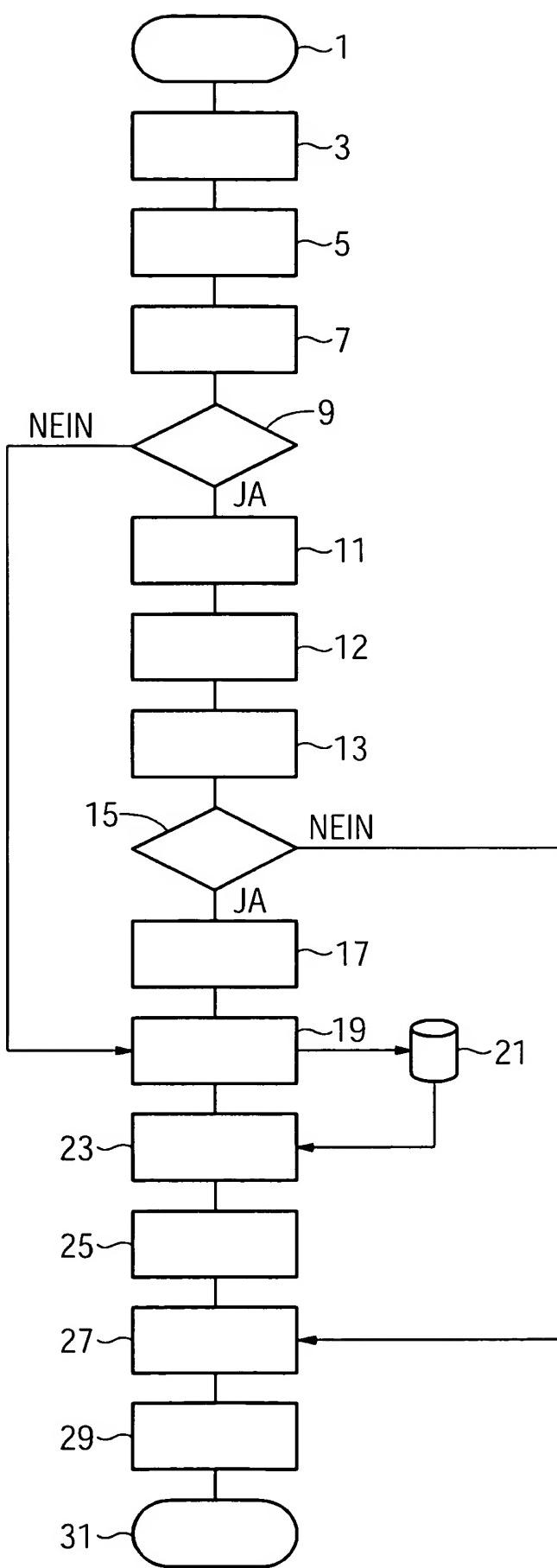
20 8. Computer-lesbares Speichermedium, auf dem Informationen  
gespeichert sind, die in Wechselwirkung mit einer Datenverar-  
beitungseinrichtung treten können, um das Verfahren nach ei-  
nem der Ansprüche 1 bis 7 auf der Datenverarbeitungseinrich-  
tung auszuführen.

## Zusammenfassung

## Verfahren zur Fernwartung technischer Einrichtungen

- 5 Die Erfindung betrifft ein Verfahren zur Fernwartung einer technischen Einrichtung (55) durch einen Wartungstechniker mittels eines Wartungsrechners (51) sowie ein computerlesbares Speichermedium, auf dem Informationen zur Ausführung des Verfahrens auf einer Datenverarbeitungseinrichtung gespeichert sind. Bei dem Verfahren wird a) in einem Schritt (3) eine Datenfernverbindung (53) zwischen dem Wartungsrechner (51) und der technischen Einrichtung (55) aufgebaut, b) in einem Schritt (11) von dem Wartungsrechner (51) eine von einem Umfang eines beabsichtigten Zugriffs auf in der technischen Einrichtung (55) gespeicherte Daten abhängige elektronische Zugriffs-Information an die technische Einrichtung (55) übermittelt, c) in einem Schritt (12) von dem Wartungsrechner (51) eine den Wartungstechniker identifizierende elektronische Kennung an die technische Einrichtung (55) übermittelt, d) in einem Schritt (15) durch die technische Einrichtung (55) in Abhängigkeit von der Zugriffs-Information und der Kennung eine Zustimmung einer Bedienperson zu einem Zugriff ermittelt und e) in einem Schritt (17) von der technischen Einrichtung (55) eine von der Ermittlung der Zustimmung abhängige elektronische Bestätigungs-Information erzeugt.

FIG 1



200303034

2/2

FIG 2

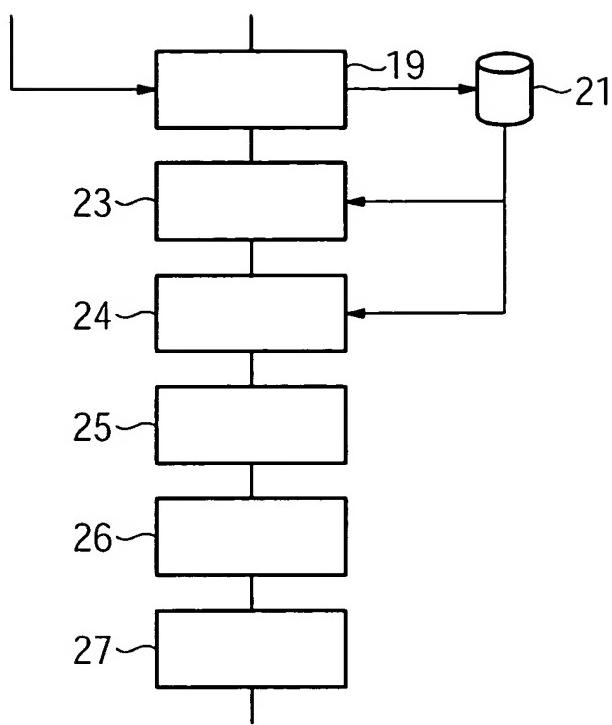
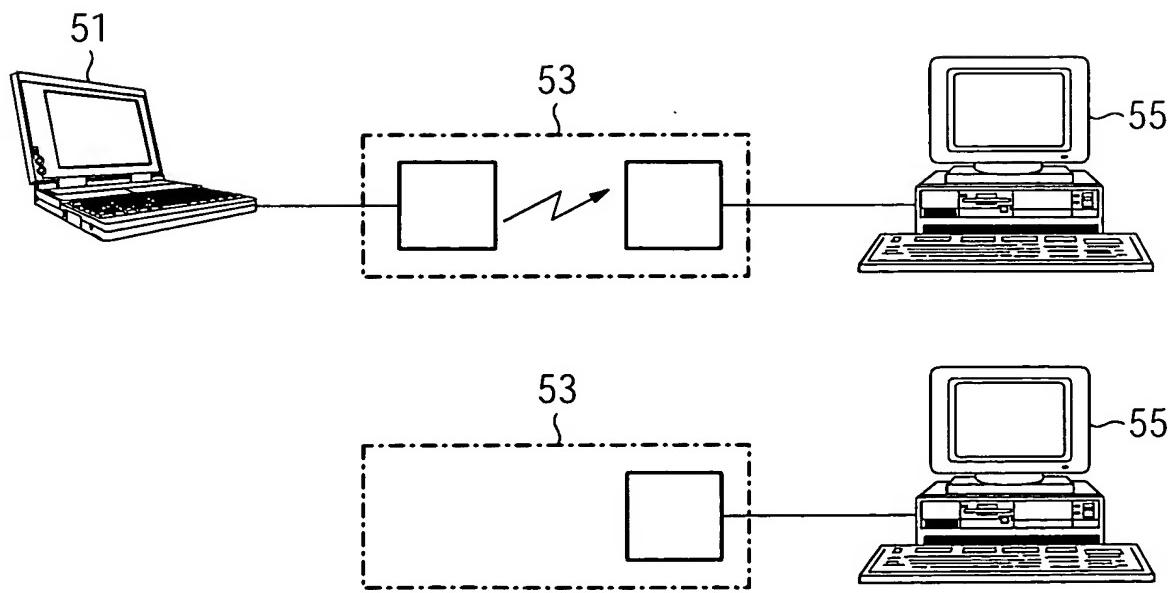


FIG 3



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TRANSLATOR'S DECLARATION AND CERTIFICATE

APPLICANT: Wesiloh et al.

SERIAL NO.: 60/457,123 GROUP ART UNIT: xxxx

FILED: March 24, 2003

TITLE: "METHOD FOR REMOTE MAINTENANCE OF  
TECHNICAL DEVICES"

Commissioner for Patents  
Box 1450  
Alexandria, VA 22313-1450

SIR:

I, Charles Bullock, declare and state that I am knowledgeable in German and English, and I hereby certify that the attached translation of German Application 103 13 271.6, filed in the German Patent and Trademark Office on 24 March 2003, is truthful and accurate to the best of my knowledge.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

DATE: 16 March 2004



**Siemens AG**  
**New Case No. P03,0118 (26965-2930)**  
**Client Reference No. 2003P03034 US**  
**Inventor: Wesiloh et al.**

## **METHOD FOR REMOTE MAINTENANCE OF TECHNICAL DEVICES**

The invention concerns a method for remote maintenance of technical devices as well as a computer-readable storage medium with a program to execute the method on a data processing device.

Technical devices such as, for example, computers, medical-technical image devices, medical workstations, industrial system controls or automobiles and airplanes are as a rule serviced by highly-specialized maintenance technicians. Maintenance measures can thereby comprise both the remedy of technical errors and the modification of the functionality. Different maintenance technicians are thereby frequently used for different maintenance measures. Additionally, maintenance technicians are specialized to different technical devices as well as to different components of devices.

The high degree of specialization makes the selection of the respectively suitable maintenance technician dependent on the respective device and on the respective necessary maintenance measure. In order to be able to implement maintenance measures quickly and flexibly, maintenance teams that implement maintenance measures via remote data connections are becoming accepted in increasing measure.

However, the remote maintenance of technical devices brings with it problems for the security of electronic data of the technical devices. On the one hand, a remote data connection that is to be established from a maintenance technician to a device to be serviced must be protected from unauthorized access by a third party. For this purpose, for example, encrypted data connections, non-public data lines or password-

protected data access can be resorted to. In all cases, the establishment of a remote data connection by one of the technical devices is only then allowed when a successful electronic identification of the connection partner has been implemented.

On the other hand, the remote maintenance brings with it the problem that a maintenance technician can in principle also obtain access to confidential data stored in the device to be serviced. Depending on the data access rights of the maintenance technician necessary for the servicing, such a possibility of access to confidential data can be an undesired side effect. The possibility of access can, however, also be necessary for maintenance and indispensable. The latter can, for example, be the case when an error behavior of the technical device can only be demonstrated by accessing confidential data.

The confidential data can, for example, be patient data, secret research papers, development information as well as know-how or demographic data. The servicing of devices that work with such data can make the access to these data necessary, however it can also make necessary only a partial access, or can be possible completely without access. The extent of the necessary data access can be estimated by the maintenance technician in the preliminary stages of a maintenance measure using the intended maintenance measure.

However, the rigid limitation of the data access rights to a previously estimated necessary scope of access would make the implementation of maintenance measures inflexible. In addition to this, a specialist that possesses sufficient knowledge of the device would have to conduct the maintenance measure on the side of the technical device in order to be able to adjust the data access rights to the scope estimated by the maintenance technician. However, as stated above, it could itself [sic] not be prevented that the access to confidential data is necessary for specific maintenance measures. The access to specific confidential data, for example patient data, can, however, be completely prohibited via legal regulations for an employee (thus, for example, for a maintenance technician from outside the company) not appointed for the work with the technical device and the confidential data.

Conventional mechanisms to monitor data access rights on the one hand do not exhibit the necessary flexibility to enable adaptations of the access rights by a non-specialist operating personnel on the side of the device to be maintained, dependent on an intended maintenance measure. This can in all cases only administrators and technical experts [sic]. On the other hand, they offer no possibility on a legal basis to enable access to data by maintenance technicians outside the firm that may not be allowed such an access based on confidential or legal regulations.

The object of the invention is to specify a method for remote maintenance of technical devices that enables a flexible regulation of data accesses by maintenance technicians under compliance with particularly strong legal limitations of data access rights.

The invention achieves this object via a method as well as via a storage medium according to the independent patent claims.

A fundamental idea of the invention is to specify a method for remote maintenance of a technical device by a maintenance technician by means of a maintenance computer, in that

- a) in a first step, a remote data connection is established between the maintenance computer and the technical device,
- b) in a further step, electronic access information dependent on a scope of intended access to data stored in the technical device is transmitted from the maintenance computer to the technical device,
- c) in a further step by the maintenance computer, an electronic identifier identifying the maintenance technician is transmitted to the technical device,
- d) in a further step by the technical device, an approval by an operating personnel of an access is determined dependent on access information and the identifier, and
- e) in a further step by the technical device, electronic authentication information is generated dependent on the determination of the approval.

The method exhibits the advantage that first a remote data connection that allows a first data access is established independent of the intended data access, based on which the scope of the intended maintenance measure and of the necessary connected data access can be planned. Dependent on this planning, the scope of the intended data access can be flexibly reacted to, in that information about this extent of data access, as well as an identification of the data accesser, is transmitted via the already existing remote data connection, based on which the approval of an operating personnel on the side of the technical device can be determined.

The approval thereby concerns not the configuration and the extent of access of the remote data connection as such, but rather the intended data access as such that should ensue by a specific maintenance technician who is in principle not designated for the work with the confidential data in question. Electronic information dependent on this approval is transmitted to the maintenance computer, whereby a particular arrangement can be made between the maintenance technician and the operating personnel that refers to the intended data access.

The materialization of this particular agreement can be designed such that particularly strong legal limitations of data access rights is [sic] thereby satisfied. For example, in this manner a work relationship between the maintenance technician and the technical device, temporally limited to the duration of the maintenance work, could be established., which enables a legitimization for the data access. The flexibility of the data access is, however, not limited, since it does not exist in the approval to adapt and allow the data access rights via technical measures corresponding to the planned maintenance extent. Rather, the approval has the character of a clarification of understanding that specially authorizes the maintenance technician for data access. For this reason, the approval can also be given by an operating personnel who is not a specialist for interaction with the technical device.

In an advantageous embodiment of the method, the authentication information is transmitted by the technical device to the maintenance computer. The

authentication information can thereby be exchanged between both parties in real time, and the agreement for maintenance purposes can quickly materialize.

In a further advantageous embodiment of the invention, information dependent on the authentication information is printed out by the technical device. This information can, for example, be printed out in the form of a written agreement that is then directly present to the operating personnel of the technical device in order, for example, for her to sign and fax to the maintenance technician. This also allows the simple and fast accomplishment of the agreement in written form.

In a further advantageous embodiment of the invention, an electronic termination information dependent on the end of the access is transmitted from the maintenance computer to the technical device. The operating personnel of the technical device can thereby be informed in real time about the end of the maintenance work. In addition to this, the end of an agreement made between maintenance technician and operating personnel for maintenance purposes can also be directly communicated and documented with the termination information. The end of the access can thereby ensue independent of a release of the remote data connection and refer only to a specified, concluded maintenance measure.

In a further embodiment of the invention, an electronic documentation of accesses effected by means of the measurement event is transmitted from the maintenance computer to the technical device. This documentation is then available at the technical device in order to make traceable the accesses of the maintenance technician to data as well as to components of the technical device. Moreover, all access to confidential data can be documented in this manner in order to be completely reconstructable after the event. This documentation can in particular serve to satisfy strong legal requirements for the documentation of data accesses to confidential data, for example patient records.

In a further advantageous embodiment of the invention, electronic data that have been transmitted from the technical device to the maintenance computer and

stored by the maintenance computer are automatically deleted by the maintenance computer from the maintenance computer dependent on a termination of the access. It can thereby be ensured that in particular confidential data, for example electronic patient records, can in fact be accessed for maintenance purposes, however do not remain at locations not provided for this after conclusion of the maintenance. The deletion of the data can serve to fulfill particularly strong legal requirements for the confidentiality and security of such data.

In a further advantageous embodiment of the invention, an extent of an intended data access is automatically determined. After establishment of the remote data connection between technical device and maintenance computer, a first error diagnosis can thereby be implemented dependent on the then [sic] a plan of the intended maintenance measure. The maintenance measure can thereby, for example, automatically be planned using the already established remote data connection, according to which a likewise automatic first error diagnosis has been implemented. However, the method can also run semi-automatically, in that a first diagnosis is effected by a maintenance technician who thereupon plans the maintenance measures intended by him by means of the maintenance computer. The automatic planning of the extent of the data access then ensues dependent on the inputs of the maintenance technician. The intended extent of the data access can thereby, for example, be associated with one or more predefined levels. Each level is thereby connected with a specific data access right.

Further embodiments of the invention result from the independent patent claims.

Exemplary embodiments of the invention are subsequently explained in detail using Figures. Thereby shown are:

FIG 1            method steps for remote maintenance,

FIG 2 method steps for automatic deletion of data in connection with remote maintenance measures, and

FIG 3 system made up of maintenance computer and technical device.

The method for remote maintenance of a technical device is shown in individual method steps in FIG 1. The maintenance method begins in step 1, in that, for example, a maintenance technician is notified by an operating personnel of a technical device. The notification can ensue via e-mail, fax or telephone. It can also be automatically generated and transmitted by the technical device 55 upon occurrence of errors.

In step 3, the maintenance technician establishes a remote data connection 53 from a maintenance computer 51 to the technical device 55 to be maintained. The remote data connection can thereby comprise a modem connection, an intranet connection, an Internet connection or another connection between the maintenance computer 51 and the technical device 55. The technical device 55 can be both a computer and another technical device with electronic control and remote data connection means.

In step 5, a first analysis of the intended maintenance measure is implemented by the maintenance technician or the maintenance computer 51. For example, an error behavior of the technical device 55 can be analyzed or a change of the configuration of the technical device 55 can be planned. The analysis can be manually implemented by the maintenance technician and be based on –information [sic] that are transmitted with the specification of the maintenance measures. The analysis can also be automatically implemented by the maintenance computer 51, which for this purpose can query configuration data, user documentations or function parameters of the technical device 55.

In step 7, the extent of the intended maintenance measure and the extent of the intended data accesses connected thereto is planned. In principle, a differentiation is

made between accesses to confidential data and accesses to non-confidential data. Maintenance measures that need no access to confidential data require no further particular precautions and can be directly implemented. In contrast to this, maintenance measures that require an access by the maintenance computer 51 to confidential electronic data require the particular approval of the possessor of the electronic data or an operating personnel authorized to access these data.

The planning of the intended scope of data accesses is thus differentiated primarily between access to confidential data and access to non-confidential data. Moreover, accesses to confidential data can differ in different extent and be correspondingly classified with regard to their extent of access. The classification can, for example, adapt to whether image data, text data, personal statements, measurement data or diagnosis data should be accessed.

In step 9, using the planning of the intended data access it is differentiated as to whether confidential data should be accessed.

In the event that confidential data is not to be accessed, the step 19 with the intended maintenance measures can be directly proceeded with.

In the event that confidential data is to be accessed, in step 11 electronic information that is dependent on the intended extent of data access is transmitted from the maintenance computer 51 to the technical device 55. This information can, for example, comprise specifications for the data to be accessed as well as for the type of the data accesses. However, it can also comprise an agreement about the intended data accesses, in the manner that a draft agreement is transmitted that contains the contractual approval of the operating personnel to an access of the maintenance technician to the confidential data. Such a contract could, for example, contain the establishment of a temporary – limited to the duration of the maintenance work – work relationship between the maintenance technician and the technical device.

In step 12, an electronic identifier that identifies the maintenance technician is transmitted from the maintenance computer 51 to the technical device 55. The identifier can either individually and unambiguously identify the maintenance technician or it can, for example, specify the role of the maintenance technician.

In step 13, the technical device 55 shows information for intended maintenance access and for the identity or role of the maintenance technician to an operating personnel via a display device, for example a monitor. In a preferred embodiment, the display comprises a pop-up window that shows an agreement that authorizes the maintenance technician for the data access in the intended extent of access.

The wording of this agreement can either have been transmitted from the maintenance computer 51 or it can be available on the side of the technical device 55. The content of the agreement can thereby be variably established dependent on the intended extent of data access, or a standard agreement, for example in the form of a document template, can be specially available for each extent of data access. In a further embodiment, instead of an agreement only information about the extent of the intended data access as well as the maintenance technician or, respectively, his role can be communicated to an operating personnel.

In step 15, the operating personnel of the technical device 55 obtains the possibility to allow the intended data access or to refuse it. The decision can be made directly on the display device of the technical device 55 via input of the approval or refusal, for example by means of keyboard or mouse. In another embodiment, the decision can be made in that the information or, respectively, the agreement shown in the preceding step is printed out by the technical device 55 and is approved in written form by an operating personnel.

In the event that the operating personnel gives no approval to the intended data access, the planned maintenance measure is cancelled in the step 27 specified below.

In the event that the operating personnel has given her approval to the data access, in step 17 an electronic signal dependent on this approval is generated that is either directly transmitted from the technical device 55 to the maintenance computer 51, or effects the generation of printout that can then, for example, be faxed.

In the event that the approval of the operating personnel has been directly input on the monitor of the technical device 55, the transmission ensues via the remote data connection 53 and can be directly displayed to the maintenance technician. In the event that the approval has been given in writing on a printout, it can be transmitted via fax or sent via post. In this case, the maintenance technician does not receive the approval or, respectively, the contractual agreement for the intended maintenance access in quite as real time as given the transmission via the remote data connection 53. This possibility can namely be used for documentation purposes, in order, for example, to centrally archive agreements or, respectively, approvals for data accesses.

In step 19, the maintenance technician undertakes maintenance measures via the already established remote data connection 53 by means of the maintenance computer 51. He thereby abides by the scope of data access previously approved by the operating personnel of the technical device 55, in order to move in the previously arranged framework of the data access. For this purpose, the remote data connection 53 does not have to be adapted and be technically limited with regard to its access possibilities; instead of this, the maintenance technician abides by the agreed extent of access.

The maintenance measures of the maintenance technician are stored in a suitable manner in a document storage 21 in order to be completely reconstructable at any time after the event.

In step 23, the information stored in the document storage 21 for documentation purposes is transmitted from the maintenance computer 51 to the

technical device 55. In particular, legal conditions for complete documentation of data accesses to confidential data can thereby be satisfied.

In step 25, the ending of the maintenance measure ensues either automatically via the maintenance computer 51 or manually by the maintenance technician. The end of the maintenance measure is thereby not identical with the release of the remote data connection 53, it means only the conclusion of the previously planned and implemented maintenance measure. Should it emerge, for example in the course of the implementation of this maintenance measure, that a data access in a changed scope is necessary, a running maintenance measure can be terminated and a maintenance measure can be commenced in the necessary, changed scope of access.

In step 27, the end of the maintenance measure is shown to an operating personnel via the technical device 55. The end of the maintenance measure is synonymous with the expiration of the approval of the operating personnel for a data access in the previously established scope. If the approval ensued in the framework of a contractual agreement, the end of the maintenance measure in step 27 is identical with the termination of the contractual agreement. For this purpose, for example a notice of termination conforming with the preceding agreement can be displayed to the operating personnel on a screen of the technical device 55.

In step 29, after the end of all maintenance measures, the remote data connection 53 is released, and in step 31 the maintenance method is ended.

The method to delete confidential data from the maintenance computer 51 is shown in FIG 2. In step 19, the implementation of maintenance measures and their storage for documentation purposes in the documentation storage 21 thereby ensues as described before. In step 23, as likewise specified before, the information stored for documentation purposes are transmitted to the technical device 55.

In step 24, the deletion of all data that have been transmitted from the technical device 55 to the maintenance computer 51 and stored by this during the

maintenance measures ensues using the information stored for documentation purposes. The use of the documentation information thereby enables the complete deletion, such that it is subsequently ensured that no confidential data remains on the side of the maintenance computer 51.

The end of the maintenance measure ensues on the side of the maintenance computer 51 in step 25, as specified before.

In step 26, the successful deletion of all confidential data that ensued previously in step 24 on the side of the maintenance computer 51 is confirmed by the operating personnel of the technical device 55 in connection with the end of the maintenance measure.

In step 27, as specified previously, the end of the maintenance measures is shown by the technical device 55 in the form of a notice of termination of the previously made agreement.

A system for maintenance of a technical device 55 is shown in FIG 3. The technical device 55 can thereby be, for example, a computer or a computer control of a device. A maintenance computer 51, for example a computer or a notebook, is connected with the technical device 55 via a remote data connection 53. The remote data connection 53 can thereby comprise a modem connection, an intranet connection, an Internet connection or other data connections. A further technical device 55 is exemplarily shown that likewise has access to a remote data connection 53, however is not connected with the maintenance computer 51.

The information necessary for execution of the method on a data processing device can be stored on a computer-readable storage medium. The storage medium can be, for example, a diskette, a diskette packet, a fixed disk, a server. The information stored thereon can interact with a data processing device in order to, for example, execute the method on the data processing device or install a program on said data processing device that is necessary for execution.

## Patent claims

1. Method for remote maintenance of a technical device (55) by a maintenance technician by means of a maintenance computer (51), in that a) in a step (3), a remote data connection (53) is established between the maintenance computer (51) and the technical device (55), b) in a step (11), electronic access information dependent on a scope of intended access to data stored in the technical device (55) is transmitted from the maintenance computer (51) to the technical device (55), c) in a step (12) an electronic identifier identifying the maintenance technician is transmitted from the maintenance computer (51) to the technical device (55), d) in a step (15), an approval by an operating personnel of an access is determined by the technical device (55) dependent on access information and the identifier, and e) in a step (17) by the technical device (55), electronic authentication information is generated dependent on the determination of the approval.
2. Method according to claim 1, in that the authentication information is transmitted from the technical device (55) to the maintenance computer (51).
3. Method according to any of the preceding claims, in that information is printed out by the technical device (55) dependent in the authentication information.
4. Method according to any of the preceding claims, in that in a step (25), electronic termination information dependent on a termination of the access is transmitted from the maintenance computer (51) to the technical device (55).
5. Method according to any of the preceding claims, in that in a step (23), an electronic documentation of accesses effected by means of the maintenance computer (51) is transmitted from the maintenance computer (51) to the technical device (55).
6. Method according to any of the preceding claims, in that in a step (24), electronic data that have been transmitted from the technical device (55) to the maintenance computer (51) and stored by this are automatically deleted from the

maintenance computer (51) by the maintenance computer (51), dependent on the termination of the access.

7. Method according to any of the preceding claims, in that an extent of the intended data access is automatically determined in a step (7).
8. Computer-readable storage medium on which is stored information that can interact with a data processing device in order to execute the method according to any of the claims 1 through 7 on the data processing device.

## **Abstract**

### **Method for remote maintenance of technical devices**

The invention concerns a method for remote maintenance of a technical device (55) by a maintenance technician by means of a maintenance computer (51) as well as a computer-readable storage medium on which is stored information for execution of the method on a data processing device. In the method, a) in a step (3), a remote data connection (53) is established between the maintenance computer (51) and the technical device (55), b) in a step (11), electronic access information dependent on a scope of intended access to data stored in the technical device (55) is transmitted from the maintenance computer (51) to the technical device (55), c) in a step (12) an electronic identifier identifying the maintenance technician is transmitted from the maintenance computer (51) to the technical device (55), d) in a step (15), an approval by an operating personnel of an access is determined by the technical device (55) dependent on access information and the identifier, and e) in a step (17) by the technical device (55), electronic authentication information is generated dependent on the determination of the approval.

**FIG**

## Reference list

- 1 begin maintenance
- 3 establish connection
- 5 error analysis
- 7 determine access level
- 9 is access to patient data necessary?
- 11 transmit employee borrowing [sic] contract
- 12 transmit maintenance technician identifier
- 13 borrowing contract pop-up at the user
- 15 transmit approval of borrowing contract
- 19 maintenance work
- 21 documentation storage
- 23 transmit documentation
- 24 delete all patient data transmitted for servicing
- 25 terminate borrowing contract
- 26 data deletion confirmation pop-up at the user
- 27 termination notice pop-up at the user
- 29 release of connection
- 31 end maintenance
- 51 maintenance computer
- 53 remote data connection
- 55 technical device

Translation / March 16, 2004 / Bullock/ 4460 words